情報セキュリティ対策基準

第10版

笛吹市

（改訂履歴）

版数	章・頁	改訂年月日	改訂内容	承認
第１版	－	平成18年4月1日	初版発行	
第２版	－	平成22年4月1日	情報セキュリティガイドラインの改定等に伴う改定	
第３版	－	平成23年4月1日	情報セキュリティガイドラインの改定等に伴う改定	
第４版	－	平成26年5月27日	情報セキュリティガイドラインの改定等に伴う改定	
第５版	－	平成28年5月24日	情報セキュリティガイドラインの改定等に伴う改定	
第６版	－	令和元年5月9日	情報セキュリティガイドラインの改定等に伴う改定	
第７版	－	令和4年4月1日	情報セキュリティガイドラインの改定等に伴う改定	
第８版	－	令和6年4月1日	情報セキュリティガイドラインの改定等に伴う改定	
第９版	－	令和7年4月1日	個人情報等の適切な取扱いを定めるための改定	
第10版	－	令和8年4月1日	情報セキュリティガイドラインの改定等に伴う改定	

目次

笛吹市情報セキュリティ対策基準

第1章　総則及び対象範囲

（目的）

第1条　笛吹市情報セキュリティ対策基準（以下「対策基準」という。）は、笛吹市情報セキュリティ基本方針（以下「基本方針」という。）に基づき、市の情報セキュリティ対策を実施するために必要となる統一的な基準を定めることにより、市の情報資産を適切に　保護することを目的とする。

（定義）

第2条　対策基準において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)　課等　市長、教育委員会の事務部局に属する課及び議会、農業委員会、監査委員、選挙管理委員会、公平委員会の事務局並びに消防本部に属する課及び消防署をいう。

(2)　サーバ等　市の情報資産のうち、サービスを提供するコンピュータ等の総称をいう。

(3)　端末　市の情報資産のうち、サーバ等からのサービスの提供を受けるコンピュータ及び事務処理のため使用するコンピュータの総称をいう。

(4)　モバイル端末　端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいう。

(5)　管理者権限　情報システムを管理するために必要なアクセス権限をいう。

(6)　情報セキュリティインシデント　望まない単独又は一連の情報セキュリティ事象及び予期しない単独又は一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

2　前項各号に規定するもののほか、対策基準において使用する用語は、基本方針、笛吹市個人情報保護法施行条例（令和4年笛吹市条例第29号）において使用する用語の例による。

（情報資産の範囲）

第3条　対策基準が対象とする情報資産は、次に掲げるとおりとする。ただし、学校教育のために小中学校で用いるものを除く。

(1)　ネットワーク、サーバ等、端末、記録媒体、情報システム及びこれらに関する設備

(2)　ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

(3)　情報システムの仕様書及びネットワーク図等のシステム関連文書

(4)　笛吹市文書管理規程（令和4年訓令第10号）第2条第1項第3号における紙文書

第2章　組織体制

（最高情報セキュリティ責任者）

第4条　市に最高情報セキュリティ責任者を置く。

2　最高情報セキュリティ責任者は、市長をもって充てる。

3　最高情報セキュリティ責任者は、市におけるすべての情報資産に対する情報セキュリティ対策の最終決定権限及び責任を有する。

（統括情報セキュリティ責任者）

第5条　市に統括情報セキュリティ責任者を置く。

2　統括情報セキュリティ責任者は、副市長をもって充てる。

3　統括情報セキュリティ責任者は、市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。また、市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

4　統括情報セキュリティ責任者は、最高情報セキュリティ責任者を補佐するとともに、情報セキュリティ責任者を統括し、情報セキュリティ対策に関する指導及び助言を行う。

5　統括情報セキュリティ責任者は、市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、最高情報セキュリティ責任者の指示に従い、又は最高情報セキュリティ責任者が不在の場合若しくは緊急時には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

（情報セキュリティ責任者）

第6条　市に情報セキュリティ責任者を置く。

2　情報セキュリティ責任者は、笛吹市庁議設置運営規程(平成30年笛吹市訓令第8号)第3条第1項第2号に規定する庁議の構成員をもって充てる。

3　情報セキュリティ責任者は、所管する組織における情報セキュリティ対策に関する統括的な権限及び責任を有する。

4　情報セキュリティ責任者は、所管する組織において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員等に対する助言及び指示を行う。

（情報セキュリティ管理者）

第6条の2　市に情報セキュリティ管理者を置く。

2　情報セキュリティ管理者は、課等の長をもって充てる。

3　情報セキュリティ管理者は、所管する組織における情報セキュリティ対策に関する権限及び責任を有する。

4　情報セキュリティ管理者は、対策基準の遵守に当たり、不明な点及び遵守困難な点に関して、適宜情報セキュリティ責任者の指示を仰ぐものとする。

5　情報セキュリティ管理者は、所管する組織に情報システムを有する場合、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

6　情報セキュリティ管理者は、所管する組織において、情報セキュリティインシデントが発生した場合又は情報セキュリティインシデントのおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及び情報セキュリティの統一的な窓口へ速やかに報告を行い、指示を仰がなければならない。

（情報セキュリティ担当者）

第6条の3　課等に、情報セキュリティ担当者を置く。

2　情報セキュリティ担当者は、当該課等の情報セキュリティ管理者が指名する。

3　情報セキュリティ担当者は、所属する課等における情報セキュリティ対策に関して情報セキュ

リティ管理者を補佐する。

4　情報セキュリティ担当者は、所属する課等に情報システムを有する場合、情報セキュリティ管理者の指示に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う。

5　情報セキュリティ担当者は、所属内における情報システム及び情報端末等の問題解決や運用に係る職員への支援を行う。また、問題解決のための窓口として情報セキュリティ管理者を補佐する

（統括情報システム責任者）

第7条　市に統括情報システム責任者を置く。

2　統括情報システム責任者は、総合政策部長をもって充てる。

3　統括情報システム責任者は、統括情報セキュリティ責任者を補佐するとともに、市における情報システム全般の情報セキュリティ対策や運用に関し、統括情報システム管理者へ助言及び指示を行う。

（統括情報システム管理者）

第7条の2　市に統括情報システム管理者を置く。

2　統括情報システム管理者は、総合政策部情報システム課長をもって充てる。

3　統括情報システム管理者は、統括情報システム責任者を補佐するとともに、市における情報システム全般の情報セキュリティ対策に関する総合的な調整を行う。

4　統括情報システム管理者は、市における情報システム、ネットワーク全般の安定稼働に努めるとともに、各課で運用する情報システムの運用支援及び総合的な調整を行う。

（統括個人情報管理者）

第8条　市に統括個人情報管理者を置く。

2　統括個人情報管理者は、総務部総務課長をもって充てる。

3　統括個人情報管理者は、市における個人情報等の適正な管理に関する総合的な調整を行う。

4　統括個人情報管理者は、各課等における個人情報等の適切な取り扱いに関する指導を行う。

（研修責任者）

第9条　市に研修責任者を置く。

2　研修責任者は、総務部総務課長をもって充てる。

3　研修責任者は、情報セキュリティに関する研修を行う権限及び責任を有する。

（情報セキュリティ委員会の開催）

第10条　最高情報セキュリティ責任者は、市における情報セキュリティに関して、重要な事項を協議する必要があるときは、笛吹市情報セキュリティ委員会設置要綱(平成18年笛吹市訓令第6号)に基づき、笛吹市情報セキュリティ委員会(以下「委員会」という。)を開催するものとする。

（兼務の禁止）

第11条　情報セキュリティ対策の実施において、承認又は許可の申請を行う者とその承認者又は許可者は、原則的として同じ者が兼務してはならない。

2　監査を受ける者とその監査を実施する者は、原則的として同じ者が兼務してはならない。

(CSIRT の設置及び役割)

第 12 条　最高情報セキュリティ責任者は、情報セキュリティインシデントに対処するための体制(CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。)を整備し、その役割を明確化しなければならない。

2　最高情報セキュリティ責任者は、CSIRTに所属する職員等を選任し、その中からCSIRT責任者を置かなければならない。また、CSIRT内の業務統括及び外部との連携等を行う職員等を定めなければならない。

3　最高情報セキュリティ責任者は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて職員等から報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

4　CSIRT は、委員会による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

5　統括情報セキュリティ責任者は、情報セキュリティインシデントを認知した場合には、その重要度及び影響範囲等を勘案し、最高情報セキュリティ責任者、総務省、県等へ報告するとともに、報道機関への通知又は公表対応を行わなければならない。

6　CSIRTは、情報セキュリティに関して、関係機関、他の地方公共団体の情報セキュリティインシデントに関する統一的な窓口の機能を有する部署及び外部の事業者等との情報共有を行わなければならない。

第 3 章　情報資産の分類と管理

(情報資産の管理責任)

第 13 条　情報セキュリティ管理者は、所管組織が作成し、及び保有する情報資産について管理責任を有する。

2　情報セキュリティ管理者は、所管する情報システムに対して、当該情報システムのセキュリティ要件に係る事項について、情報システム台帳を整備しなければならない。

3　情報セキュリティ管理者は、情報資産が複製された場合の所在を明確にしておかなければならない。

(情報資産の分類)

第 14 条　市のすべての情報資産は、別表 1 に掲げる重要性分類に基づき、次に掲げるとおり分類しなければならない。

(1)　重要性分類 A　機密保持を要する情報が含まれており、情報セキュリティ侵害によって市民又は行政に重大な影響を及ぼすおそれがある情報資産

(2)　重要性分類B　情報セキュリティ侵害によって市民又は行政に影響を及ぼすおそれがある情報資産

(3)　重要性分類C　公開情報等であり、情報セキュリティ侵害による市民又は行政への影響がほとんどない情報資産

2　情報セキュリティ管理者は、所管組織の保有する情報について、前項の分類に従った重要性分類を行わなければならない。

3　情報セキュリティ管理者は、必要に応じて、所管組織において取り扱う情報資産について、重要性分類に応じた取扱制限についても明示する等適切な管理を行わなければならない。

（情報資産の作成）

第 15 条　職員等は、業務上必要のない情報資産を作成してはならない。

2　情報セキュリティ管理者は、作成した情報資産について、施錠管理及びアクセス制限等、情報資産の重要性分類に従った取扱制限を講じなければならない。

3　情報資産を作成した者は、文書、ファイル及び収納する記録媒体に情報資産の分類を表示し、必要に応じて取扱制限を明示する等適正な管理を行わなければならない。

4　情報資産を作成する者は、作成途上の情報資産についても、紛失や流出等を防止しなければならない。また、情報資産の作成途上で不要になった場合は、当該情報資産を消去しなければならない。

（情報資産の入手）

第 16 条　庁内の職員が作成した情報資産を入手した職員は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

2　庁外の者が作成した情報資産を入手した職員は、第 14 条第 1 項の分類に従い、当該情報の分類と取扱制限を定めなければならない。

3　情報資産を入手した職員は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

（情報資産の利用）

第 17 条　職員等は、業務以外の目的に情報資産を利用してはならない。

2　情報資産を利用するときは、第 14 条第 1 項の分類に応じ、適正に利用しなければならない。

3　情報資産を利用する職員等は、記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。

4　職員等は、重要性分類 A に該当する情報資産のうち電磁的に記録されたものについては、必要に応じて情報システム課に依頼し、暗号化を施して管理しなければならない。

5　職員等は、情報資産を記録した記録媒体を長期保管する場合は、書込禁止等の措置を講じなければならない。

（情報資産の保管）

第 18 条　情報セキュリティ管理者は、第 14 条第 1 項の分類に従って、情報資産を適正に保管しなければならない。

2　情報セキュリティ管理者は、利用頻度が低い記録媒体や情報システムのバックアップで取得したデータを記録する記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。

3　情報セキュリティ管理者は、重要性分類Ｂ以上の情報資産を記録した記録媒体を保管する場合、可能な限り耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

4　情報資産の保存年限については、笛吹市文書管理規程（平成 16 年笛吹市訓令第 6 号）等により定めのあるものを除き、情報セキュリティ管理者が定める。

（情報資産の送信）

第 19 条　ネットワーク等を用いて情報資産を伝送する場合は、情報資産を伝送するシステムを所管する課等の情報セキュリティ管理者が、当該情報資産が安全かつ確実に伝送されるよう、必要に応じて通信の暗号化等の対策を講じなければならない。

（情報資産の運搬及び持出し）

第 20 条　職員等は、重要性分類 B 以上の情報資産を市が管理するネットワーク及び施設の外（以下「外部」という。）へ運搬してはならない。ただし、次に掲げる情報資産に関しては、この限りではない。

(1)　法令等の規定に従い開示する情報資産

(2)　前号を除き、情報セキュリティ管理者が許可した情報資産

2　情報セキュリティ管理者は、情報資産の運搬を行う場合、次に掲げるとおり管理しなければならない。

(1)　信頼できる者の選任

(2)　管理簿等による持出し管理

3　職員等は、情報資産を外部に持ち出す場合、次に掲げるとおり管理しなければならない。

(1)　施錠可能な場所への収納の徹底

(2)　外部における放置禁止の徹底

4　職員等は、外部に持ち出した情報資産を紛失した場合、直ちに第116条の緊急時対応計画に従って報告を行わなければならない。

（情報資産の提供及び公開）

第 21 条　重要性分類Ｂ以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

2　前項により重要性分類Ｂ以上の情報資産を外部に提供する者は、
暗号化又はパスワードの設定を行わなければならない。

3　情報セキュリティ管理者は、市民に公開する情報資産について、完全性を確保しなければならない。

（情報資産の廃棄）

第 22 条　職員等は、情報資産の廃棄に関し、情報セキュリティ管理者の許可を得たうえで、重要性分類に応じて次に掲げる事項を実施しなければならない。

(1)　廃棄する情報資産の数量を確認すること。

(2)　記録媒体に含まれる情報資産は、復元できないように対処した上で廃棄すること。

(3)　紙媒体の情報資産を廃棄する場合は、裁断機等で細かく裁断し、内容が確認できないようにすること。

(4)　記録媒体の廃棄を行う場合、行った処理について、日時、処理実施者及び処理内容を記録しなければならない。

(5)　委託事業者に廃棄を委託する場合は、機密保持について契約書に明記すること。

第 4 章　情報システム全体の強靭性の向上

（マイナンバー利用事務系）

第 23 条　個人番号利用事務（社会保障、税及び災害対策等において、保有している個人情報の検索や管理のためにマイナンバーを利用する特定の事務のこと）又は戸籍事務等に関わる情報システム及びデータ（以下「マイナンバー利用事務系」という。）は、他の領域と通信できないようにしなければならない。

2　マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。この場合において、相手先となる外部の接続先もインターネット等と接続してはならない。

3　前項において、例外として国等の公共機関が構築したシステム等、十分に安全性が確保された外部接続先については、LGWAN を経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

4　マイナンバー利用事務系については、情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。また、業務ごとに専用端末を設置することが望ましい。

5　マイナンバー利用事務系については、原則として、USB メモリ等の記録媒体による端末からの情報の持出しができないように設定しなければならない。

（LGWAN 接続系）

第 24 条　LGWAN への接続が可能なネットワークで、業務に利用する情報システム及びその情報システムで取り扱うデータ（以下「LGWAN 接続系」という。）について、LGWAN 接続系とインターネットメール、ホームページ管理システム等に関するインターネットに接続された情報システム及びその情報システムで取り扱うデータ（以下「インターネット接続系」という。）は、両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次に掲げる方式等により、無害化通信を図らなければならない。

(1)　インターネット環境で受信したインターネットメールの本文のみをテキスト化し、LGWAN 接続系に転送する方式

(2)　インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

(3)　インターネット環境で受信又はダウンロードしたデータから不正プログラム等を除去したうえで LGWAN 接続系に取り込む方式

（インターネット接続系）

第 25 条　インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

2　県及び市町村のインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、総務省や県等と連携しながら、情報セキュリティ対策を推進しなければならない。

第5章　物理的セキュリティ

第1節　サーバ等の管理

(機器の取付け)

第26条　情報セキュリティ管理者は、サーバ等、端末及びその他機器を取付ける場合、次に掲げる事項を実施しなければならない。

(1)　温度、湿度、埃及び振動等の影響を可能な限り排除すること。

(2)　既存の情報システムに対する影響について確認すること。

(3)　サーバ室に機器を設置できない場合、重要性に応じて機器への鍵の取付け等の措置を講じること。

(サーバ等の冗長化)

第27条　情報セキュリティ管理者は、サーバ等の障害発生時における情報資産等の滅失及び情報システムの運用停止を回避するため、情報システムの業務内容及び保有する情報資産の重要度に応じて、サーバ等を冗長化(二重化等)しなければならない。

(機器の電源)

第28条　情報セキュリティ管理者は、サーバ等の電源を適正に管理するため、次に掲げる事項を実施しなければならない。

(1)　電力供給の停止後、サーバ等が正常に動作を終了するまでの間、必要な予備電源を備えること。

(2)　落雷による過電流からサーバ等を保護するための措置を講じること。

(3)　電源プラグが簡単にはずれないよう、可能な限り必要な措置を講じること。

(通信ケーブル等の配線)

第29条　情報セキュリティ管理者は、通信ケーブル等の配線を適正に管理するため、次に掲げる事項を実施しなければならない。

(1)　配線が損傷しないよう、床下への配線又は保護カバーの取付けを行うこと。

(2)　相互干渉による障害を防止するために、電源ケーブルを通信ケーブルから隔離して配線する等、可能な限り必要な処置を講ずること。

(3)　配線の損傷を把握するため、必要に応じて点検を行うこと。

2　統括情報システム管理者は、ハブのポート等ネットワーク接続口を他者が容易に接続できない措置を講じる等適正に管理しなければならない。

(機器の定期保守及び修理)

第30条　情報セキュリティ管理者は、サーバ等の機器の定期保守を実施しなければならない。

2　情報セキュリティ管理者は、記録媒体を内蔵する機器を委託事業者に修理させる場合、記録内容を消去した状態で行わせなければならない。

3　前項において記録内容を消去できない場合、情報セキュリティ管理者は、事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

4　情報セキュリティ管理者は、契約により操作を認めた委託事業者以外の者が、配線を変更又は追加できないように必要な措置を講じなければならない。

(庁外への機器の設置)

第 31 条　情報セキュリティ管理者は、庁外にサーバ等の機器を設置する場合、最高情報セキュリティ責任者及び統括情報システム管理者の承認を得なければならない。

2　前項において情報セキュリティ管理者は、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

(機器の廃棄等)

第 32 条　情報セキュリティ管理者は、機器を廃棄する場合、機器に保存されている情報の消去等を行い、当該情報が復元不可能な状態にしなければならない。

2　情報セキュリティ管理者は、委託事業者に機器の廃棄を委託する場合、機密保持について契約書に明記しなければならない。

3　情報セキュリティ管理者は、貸借した機器を返却する場合、機器に保存されている情報の消去等を行い、当該情報が復元不可能な状態にしなければならない。ただし、賃貸借契約等において機密保持及び返却時における情報の確実な消去について明記されている場合は、この限りではない。

第 2 節　管理区域(サーバ室)の管理

(管理区域の構造等)

第 33 条　統括情報セキュリティ責任者及び統括情報システム管理者は、重要性分類 A の区分に該当する情報資産を取り扱うシステム等を設置する場合、原則として外部からの侵入が容易にできないよう外壁等に囲まれた管理区域(以下「サーバ室」という。)に設置しなければならない。

2　統括情報セキュリティ責任者及び統括情報システム管理者は、サーバ室の情報セキュリティ対策を次に掲げるとおり実施しなければならない。

(1)　サーバ室に設置された外部に通ずるドアは、許可されていない立入りを防止するための制御機能、鍵及び警報機能等を導入すること。

(2)　サーバ室には、内部で作業する者を監視する機能を設置すること。

(3)　サーバ室は、耐震対策及び防火措置を講じるほか、可能な限り防水及び外部からの電磁波の影響の排除等を行うこと。

(4)　サーバ室の消火方法は、機器及び記録媒体等に影響を与えないものを使用すること。

(5)　サーバ室内の温度及び湿度を調整する装置を設置すること。

(サーバ室の入退室管理等)

第 34 条　統括情報システム管理者は、サーバ室への入退室に関して、次に掲げるとおり管理しなければならない。

(1)　サーバ室の利用者を登録及び削除する手順を作成すること。

(2)　ICカード又は生体認証装置等による利用者認証及び入退室管理簿の記載による入退室管理を行うこと。

(3)　サーバ室では、身分証明書を確認できるように着用させること。

(4)　サーバ室に設置された情報システムに関連しない端末、通信回線装置又は記録媒体等を持ち込ませないようにすること。

(機器等の搬出入)

第35条　統括情報システム管理者は、サーバ室に搬入する機器等が、既存の情報システムに与える影響について、あらかじめ当該情報システムを所管する情報セキュリティ管理者又は委託事業者に確認を行わせなければならない。

2　統括情報システム管理者は、サーバ室の機器等の搬出入の際に、搬出入する情報システムを所管する課等の職員を立ち会わせなければならない。

第3節　通信回線及び通信回線装置の管理

(通信回線等の管理)

第36条　統括情報セキュリティ責任者は、庁内の通信回線、通信回線装置及びこれらに関連する図書を適正に管理しなければならない。

2　統括情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。

3　統括情報セキュリティ責任者は、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

4　最高情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク(LGWAN)に集約するように指示しなければならない。

5　情報セキュリティ管理者は、重要性分類B以上の情報資産を取り扱うシステムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。

6　情報セキュリティ管理者は、ネットワークに使用する回線について、伝送途上に情報資産の破壊、盗聴、改ざん又は消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。

7　統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。

8　情報セキュリティ管理者は、重要性分類B以上の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択するとともに、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

第4節　事務室等における端末等の管理

(端末及び記録媒体の管理)

第37条　情報セキュリティ管理者は、執務等を行う場所(以下「事務室等」という。)に設置した端末に対して、盗難防止のための物理的な措置を次に掲げるとおり施さなければならない。

(1)　セキュリティワイヤーによる端末の固定

(2)　モバイル端末の施錠可能な場所への収納

2　情報セキュリティ管理者は、記録媒体に情報を保存する必要がなくなったときは、速やかに記録した情報を消去した上で保管しなければならない。

3　事務室等における部外者の侵入等による情報資産の盗み見や不正持ち出し等の防止のための物理的な情報セキュリティ対策は、各施設の管理責任者及び情報セキュリティ管理者が行わな

ければならない。

4　情報セキュリティ管理者は、職員等が利用する端末等に情報システムへのログインパスワードの入力を必要とするように設定しなければならない。

5　情報セキュリティ管理者は、マイナンバー利用事務系の情報システムについては、「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証等）を行うよう設定しなければならない。

第6章　人的セキュリティ

第1節　職員等の遵守事項

（職員等の責務）

第38条　職員等は、情報セキュリティ対策の実施に当たり、次に掲げる責務を有する。

(1)　情報セキュリティポリシー及び実施手順に定められている事項を遵守すること。

(2)　情報セキュリティポリシー及び実施手順について不明な点又は遵守することが困難な点がある場合は、速やかに情報セキュリティ管理者に報告し、指示等を仰ぐこと。

(3)　不適切な情報の発信又は利用を許可されていない情報資産へのアクセス等、自らが加害者になる行為を行わないこと。

（情報資産の目的外利用の禁止）

第39条　職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセス等を行ってはならない。

2　統括情報セキュリティ責任者は、業務以外の目的で情報資産の利用を行った職員等に対して、職員等が所属する情報セキュリティ管理者を通じて、中止及び改善を指導しなければならない。

（情報資産を外部で処理する場合の安全管理措置）

第40条　最高情報セキュリティ責任者は、重要性分類Ｂ以上の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

2　職員等は、重要性分類Ｂ以上の情報資産を外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

3　職員等は、外部で重要性分類Ｂ以上の情報を処理する場合には、情報セキュリティ管理者の許可を得なければならない。

4　職員等は、外部に持ち出す情報資産を紛失した場合、直ちに緊急時対応計画に従って報告を行わなければならない。

（支給以外の端末等の業務への使用の禁止）

第41条　職員等は、支給以外の端末及び記録媒体等を原則業務に使用してはならない。ただし、特別の理由がある場合には、統括情報システム管理者の許可を得て使用することができる。

2　重要性分類Ｂ以上の情報資産については、支給以外の端末及び記録媒体等による情報処理を行ってはならない。

（端末等の持ち出し等の記録）

第42条　情報セキュリティ管理者は、端末及び記録媒体等の持ち出し及び持ち込みについて記録を作成し、保管しなければならない。

（ソフトウェアのセキュリティ機能の設定変更の禁止）

第 43 条　職員等は、端末のソフトウェアに関するセキュリティ機能の設定を統括情報システム管理者の許可なく変更してはならない。

（机上の端末等の管理）

第 44 条　職員等は、端末、記録媒体及び情報が印刷された文書等について、第三者に使用され、又は情報を閲覧されることのないよう、次に掲げる措置を講じなければならない。

(1)　端末を離席時にログアウトする。

(2)　端末に画面ロックを設定する。

(3)　記録媒体及び文書等が容易に閲覧されない場所へ保管する。

2　職員等は、コピー機、ファクシミリ又はプリンタ等に入出力書類を放置してはならない。

（ウェブ及び電子メール等の利用）

第 45 条　職員等は、業務以外の目的でウェブを閲覧してはならない。

2　職員等は、電子メール等の利用において、次に掲げる事項を遵守しなければならない。

(1)　私的に利用している電子メールアドレス宛てに、業務上の電子メールを転送しないこと。

(2)　電子メール及びファクシミリを送信する場合、宛先を必ず確認し、誤送信を防止すること。

(3)　外部のメーリングリストに参加する場合、業務への必要性を十分考慮した上で参加するとともに、公序良俗に反する発言をしないこと。

(4)　複数人に電子メールを送信するときは、必要がある場合を除き、BCC 等により他の送信先の電子メールアドレスが分からないようにすること。

(5)　送信可能な電子メールの容量等の制限事項を遵守すること。

3　職員等は、ウェブで利用できるフリーメール等を使用してはならない。

4　大容量ファイルの授受を行うため、ネットワークストレージサービスを利用する場合には、情報セキュリティ管理者はその安全性を確認し統括情報システム管理者の承認を得る。

（退職時等の遵守事項）

第 46 条　職員等は、異動又は退職等により業務を離れる場合には、利用していた情報資産を返却するとともに、業務上知り得た情報を漏らしてはならない。

（会計年度任用職員等への対応）

第 47 条　情報セキュリティ管理者は、臨時的任用職員、再任用職員及び会計年度職員等に情報資産を利用させる場合は、採用時に情報セキュリティポリシー及び実施手順等のうち、臨時的任用職員、再任用職員及び会計年度職員等が守るべき内容を理解させ、実施及び遵守させる等、適切な指導を行わなければならない。

2　情報セキュリティ管理者は、臨時的任用職員、再任用職員及び会計年度職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

3　情報セキュリティ管理者は、臨時的任用職員、再任用職員及び会計年度職員等に端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

4　情報セキュリティ管理者は、臨時的任用職員、再任用職員及び会計年度職員等に、端末で取り扱うことができる情報資産を制限しなければならない。

（情報セキュリティポリシー等の閲覧）

第 48 条　情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるようにしなければならない。

（委託事業者の指導）

第 49 条　情報セキュリティ管理者は、ネットワーク及び情報システムの開発及び保守等を委託事業者に発注する場合、委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち委託事業者が遵守すべき事項及び機密事項について説明し、情報資産の利用に関する適切な指導を行わなければならない。

第 2 節　研修及び訓練

（情報セキュリティに関する研修及び訓練）

第 50 条　最高情報セキュリティ責任者は、すべての職員等に対し、情報セキュリティに関する研修及び訓練を行わなければならない。

（情報セキュリティに関する研修計画の策定及び実施）

第 51 条　研修責任者は、次に掲げる研修について、研修計画の策定とその実施体制の構築を行い、委員会の承認を得なければならない。

(1)　情報セキュリティ責任者及び情報セキュリティ管理者に必要な知識及び技術の習得に資するための研修

(2)　情報セキュリティ担当者に必要な知識及び技術の習得に資するための研修

(3)　職員等に必要な知識の習得に資するための階層別研修

2　情報セキュリティ管理者は、所管する情報システムの利用者に、研修を受講させなければならない。

（研修結果の評価及び見直し）

第 52 条　研修責任者は、アンケート調査等により、研修を受講した者が目標とする水準に達したかどうか評価を行わなければならない。

2　研修責任者は、前項の結果により、必要に応じて研修の内容を見直さなければならない。

（緊急時を想定した訓練）

第 53 条　統括情報セキュリティ責任者は、緊急時対応計画に基づき、情報セキュリティインシデント発生時に CSIRT が適切に機能するよう、情報セキュリティインシデントの発生を想定した緊急時対応訓練を年に 1 回以上実施しなければならない。

2　前項に規定する訓練は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の内容及び範囲等を定め、効果的に実施できるようにしなければならない。

（研修及び訓練への参加）

第 54 条　幹部を含めた全ての職員等は、定められた研修及び訓練に参加しなければならない。

第 3 節　情報セキュリティインシデントの報告

（庁内での事故等の報告）

第 55 条　職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

2　報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報セキ

ュリティ責任者に報告しなければならない。

3　情報セキュリティ管理者は、報告を受けた情報セキュリティインシデントに関して、緊急時対応計画に従って適切に対処しなければならない。

4　情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ報告しなければならない。

(外部からの事故の報告)

第 56 条　職員等は、市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、市民等外部から情報の提供を受けた場合、情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

2　情報セキュリティ管理者は、報告を受けた情報セキュリティインシデントに関して、緊急時対応計画に従って適切に対処しなければならない。

(情報セキュリティインシデントに係る原因の究明、記録及び再発防止等)

第 57 条　CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

2　CSIRT は、情報セキュリティインシデントであると評価した場合、最高情報セキュリティ責任者に速やかに報告しなければならない。

3　CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ管理者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。また、CSIRT は、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報セキュリティ管理者へ確認を指示しなければならない。

4　CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、最高情報セキュリティ責任者に報告しなければならない。

5　最高情報セキュリティ責任者は、CSIRT から情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

第 4 節　ID 及びパスワード等の管理

(認証用 IC カード等の取扱い)

第 58 条　職員等は、認証に用いる IC カード等を、次に掲げるとおり、厳重に管理しなければならない。

(1)　個人認証に用いる IC カード等を紛失しないよう、適切に管理すること。

(2)　個人認証に用いる IC カード等を貸与しないこと。

(3)　所属認証に用いる IC カード等を使用する場合は、情報セキュリティ管理者の許可を得ること。

(4)　IC カード等は、必要のないときにカードリーダ又は端末等のスロット等から抜くこと。

(5)　個人又は所属認証に用いる IC カード等は、紛失若しくはき損をした場合又は盗難若しくは詐取にあった場合、直ちに情報セキュリティ管理者に報告すること。

2　情報セキュリティ管理者は、認証に用いる IC カード等について、次に掲げるとおり管理しなければならない。

(1)　所属認証に用いる IC カード等を厳重に管理すること。

(2)　職員等の個人認証に用いる IC カード等の管理状況を管理すること。

(3)　職員等から IC カード等の紛失、き損、盗難又は詐取等の報告を受けた場合、直ちに該当する IC カード等の利用を無効とする措置を講じること。

3　情報セキュリティ管理者は、ICカード等を切り替える場合、切替え前のカードを回収し、破砕する等復元不可能な処理を行った上で廃棄しなければならない。

(ID の取扱い)

第 59 条　職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

(1)　自己が利用している ID は、他人に利用させてはならない。

(2)　共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

(パスワードの取扱い)

第 60 条　職員等は、自己の保有するパスワードに関し、第三者に漏えいしないよう、次に掲げるとおり、厳重に管理しなければならない。

(1)　パスワードを秘密にしておくこと。

(2)　パスワードのメモを作成した場合は、端末に貼り付けない等、第三者の目に触れることがないよう適切に管理すること。

(3)　パスワードは、十分な長さを保つこと。

(4)　パスワードには、辞書等に記載されている単語又は生年月日等、第三者に推測されやすいものを設定しないこと。

(5)　パスワードが漏えいしたおそれがある場合には、情報セキュリティ管理者に報告し、速やかにパスワードを変更すること。

(6)　パスワードは定期的に変更すること。

(7)　複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いないこと。

(8)　仮のパスワード（初期パスワードを含む）は、最初のログイン時点で変更すること。

(9)　端末にパスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。

(10)　職員等の間でパスワードを共有しないこと。(課等における共有 ID に対するパスワードを除く。)

2　情報セキュリティ管理者は、所管組織で共有するパスワードに関し、前項のとおり厳重に管理しなければならない。

第 7 章　技術的セキュリティ

第 1 節　コンピュータ及びネットワークの管理

(文書サーバの設定等)

第 61 条　統括情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

2　統括情報システム管理者は、文書サーバを課等の単位で構成し、職員等が他の課等のフォルダ及びファイルを閲覧及び利用できないように、設定しなければならない。

3　統括情報システム管理者は、市民の個人情報、人事記録及び特定の職員しか取り扱えないデータについて、別途フォルダを作成する等の措置を講じ、同一課等内であっても、担当職員以外の職員等が閲覧及び利用できないように設定しなければならない。

(バックアップの実施)

第 62 条　情報セキュリティ管理者は、サーバ等に記録された情報について、サーバの冗長化対策にかかわらず、必要に応じて定期的にバックアップを実施しなければならない。

2　情報セキュリティ管理者は、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。

3　情報セキュリティ管理者は、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

(システム変更作業の記録及び作業内容の確認)

第 63 条　情報セキュリティ管理者は、情報システムの変更等を行う場合、次に掲げる事項を実施しなければならない。

(1)　作業の記録を作成し、詐取又は改ざん等をされないように適正に管理すること。

(2)　運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直しをすること。

(3)　情報システムの運用に大きな影響を及ぼす可能性がある作業を行う場合は、2 名以上で作業を行い、相互に作業内容を確認すること。

(情報システム仕様書等の管理)

第 64 条　情報セキュリティ管理者は、所管する情報システムに関する仕様書及びネットワーク構成図等(以下「構成図等」という。)を、次に掲げるとおり管理しなければならない。

(1)　構成図等は常に最新の状態に整備すること。

(2)　構成図等を業務上必要とする者以外の者が閲覧し、又は紛失すること等がないよう、適正に管理すること。

(ログの取得等)

第 65 条　統括情報システム管理者及び情報セキュリティ管理者は、次に掲げるとおり、ログ等の取得及び管理を行わなければならない。ただし、統括情報セキュリティ責任者が不要と判断した情報システムについては、この限りではない。

(1)　ネットワーク機器及びサーバ等のログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存すること。

(2)　ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処方法について事前に定めておくこと。

(3)　定期的にサーバ等のログ等を確認し、悪意ある第三者等からの不正侵入又は不正操作等の有無について、点検及び分析を実施すること。

2　情報セキュリティインシデントへの対策を検討するため、委員会から指名された者は、ログ等

の閲覧及び調査をすることができる。

（障害記録）

第 66 条　情報セキュリティ管理者は、情報システムの障害に対する処理を体系的に記録し、必要な時に活用できるよう管理しなければならない。

（ネットワークの接続制御及び経路制御等）

第 67 条　統括情報システム管理者は、フィルタリング及びルーティングに不整合が発生しないように、ファイアウォール及びルータ等の通信ソフトウェア等を設定しなければならない。

2　統括情報システム管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

3　保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保しなければならない。また、情報セキュリティ対策について、定期的な確認により見直さなければならない。

（外部の者が利用できるシステムの分離等）

第 68 条　統括情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離し、又は情報セキュリティ上の問題が生じないよう論理的に分離する等の措置を講じなければならない。

（外部ネットワークとの接続制限等）

第 69 条　情報セキュリティ管理者は、外部のネットワークと接続を行う場合、あらかじめ最高情報セキュリティ責任者に申請し許可を得なければならない。

2　最高情報セキュリティ責任者は、前項により申請のあったものについて、外部のネットワークの情報セキュリティ対策の実施状況並びに市のネットワーク及び情報システムへの影響等について調査しなければならない。

3　情報セキュリティ管理者は、外部ネットワークとの接続を行った場合、適切な情報セキュリティ対策及び運用管理を行わなければならない。

4　情報セキュリティ管理者は、庁外にサーバ等を設置し外部ネットワークにより接続する場合、その設置場所について、最高情報セキュリティ責任者に申請し許可を得なけなければならない。

5　情報セキュリティ管理者は、当該設置場所における物理的安全対策を調査しなければならない。

6　情報セキュリティ管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

7　統括情報システム管理者及び情報セキュリティ管理者は、ウェブサーバ等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。

(1)　庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置したうえで接続しなければならない。

(2)　脆弱性が存在する可能性が増大することを防止するため、ウェブサーバが備える機能のうち、必要な機能のみを利用しなければならない。

(3)　ウェブサーバからの不用意な情報漏えいを防止するための措置を講じなければならない。

(4)　情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定しなければならな

い。

8　統括情報システム管理者及び情報セキュリティ管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

(複合機のセキュリティ管理)

第 70 条　情報セキュリティ管理者は、プリンタ複合機(以下「複合機」という。)を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じた適切なセキュリティ要件を満たしていることの確認を、統括情報システム管理者から受けなければならない。

2　統括情報システム管理者は、複合機が備える機能について適正な設定等を行うことにより、運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

3　情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ記録媒体の全ての情報を消去し、又は再利用できないようにする対策を講じなければならない。

(IoT 機器を含む特定用途機器のセキュリティ管理)

第 71 条　テレビ会議やネットワークカメラ等の特定の用途に使用される情報システム（以下「特定用途機器」という。）について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

(無線 LAN のセキュリティ対策及びネットワークの盗聴対策)

第 72 条　情報セキュリティ管理者は、無線 LAN を使用する場合、統括情報セキュリティ責任者の許可を得なければならない。

2　統括情報セキュリティ責任者は、無線LANの利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

3　統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

(電子メールのセキュリティ管理)

第 73 条　統括情報システム管理者及び情報セキュリティ管理者は、メールサーバを運用する場合、次に掲げる事項を実施しなければならない。

(1)　権限のない利用者による不正な利用が行われないようにすること。

(2)　容量の非常に大きい電子メール等、他の情報システムに悪影響を与えるおそれのある電子メールの送受信を不可能とすること。

2　統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

3　統括情報セキュリティ責任者は、職員等が利用する電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

4　統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことを抑止できるように、システム上の措置を講じなければならない。

（電子署名及び暗号化）

第 74 条　情報セキュリティ管理者は、電子署名及び暗号化の方法並びに暗号化に使用する鍵の管理方法について、適切な手順を定めなければならない。

2　職員等は、情報資産の分類により定めた取扱制限に従い、外部に送信する添付ファイル等の情報資産について、機密性又は完全性を確保する必要がある場合には、前項に定められた手順により電子署名、暗号化又はパスワード設定を使用して送信しなければならない。

3　最高情報セキュリティ責任者は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（無許可ソフトウェアの導入等の禁止）

第 75 条　統括情報セキュリティ責任者は、業務において使用するソフトウェアを定めなければならない。

2　職員等は、定められたソフトウェア以外のソフトウェアを端末に導入してはならない。ただし、業務上特別の理由がある場合には、統括情報セキュリティ責任者及び統括情報システム管理者の許可を得ることにより導入することができる。

3　前項ただし書きにおいて、情報セキュリティ管理者は、導入するソフトウェアのライセンスを管理しなければならない。

（端末等の改造及び設定変更の制限）

第 76 条　職員等は、端末及びネットワーク機器に対し、改造及び設定の変更を行ってはならない。ただし、業務上特別の理由がある場合には、統括情報システム管理者及び情報セキュリティ管理者の承認を得て行うことができる。

（無許可でのネットワーク接続の禁止）

第 77 条　職員等は、許可なく端末及び記録媒体等をネットワークに接続してはならない。ただし、特別の理由がある場合には、統括情報システム管理者の許可を得て接続することができる。

（業務以外の目的でのウェブ利用等の禁止）

第 78 条　統括情報セキュリティ責任者及びウェブ利用に関する管理者権限を持つ者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを確認した場合は、情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

2　統括情報セキュリティ責任者及びウェブ利用に関する管理者権限を持つ者は、ウェブで利用できる電子メール、ネットワークストレージサービス等の利用を禁止する措置を講じなければならない。

（Web 会議サービスの利用時の対策）

第79条　統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。

2　職員等は、市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施しなければならない。

3　職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策しなければならない。

4　職員等は、外部からWeb 会議に招待される場合は、市の定める利用手順に従い、必要に応じ

て利用申請を行い、承認を得なければならない。

（ソーシャルメディアサービスの利用）

第80条　統括情報セキュリティ責任者は、市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用規定を定めなければならない。

(1)　市のアカウントによる情報発信が、実際の市のものであることを明らかにするために、市の公式ホームページに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

(2)　パスワードや認証のためのコード等の認証情報及びこれを記録した媒体(IC カード等)等を適正に管理するなどの方法で、不正アクセス対策を行うこと。

2　前項において、ソーシャルメディアサービスを利用する場合は、重要性分類Ｂ以上の情報を発信してはならない。

3　第1項においてソーシャルメディアサービスを利用する場合は、利用するソーシャルメディアサービスごとの責任者を定めなければならない。

4　市のアカウントの乗っ取り及び市のアカウントへのなりすましを確認した場合、被害を最小限にするための措置を講じなければならない。

第２節　アクセス制御

(アクセス制御)

第 81 条　統括情報システム管理者又は情報セキュリティ管理者は、次に掲げるとおり、サーバ等におけるアクセス制御を行わなければならない。

(1)　所管するサーバ等のアクセス権限を明確にし、アクセス権限に基づくアクセス制御を行うこと。

(2)　サーバ等の設定に関する情報及びログ等は、原則として管理者権限を持つ者のみが参照できること。

(3)　サーバ等及びネットワーク機器において、出荷時に提供される通信を行うための機能のうち、使用しないものを削除し、又は停止すること。

(4)　サーバ等及びネットワーク機器において、機器固有情報によるアクセス制御を行うこと。

2　統括情報システム管理者又は情報セキュリティ管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

(利用者 ID の取扱い)

第 82 条　統括情報システム管理者及び情報セキュリティ管理者は、所管する情報システムにおける利用者 ID の管理に関して、次に掲げる手順を定めなければならない。

(1)　利用者 ID の新規登録、変更及び削除等における申請及び管理手順

(2)　利用者の異動、出向及び退職等における利用者 ID の取扱い手順

2　統括情報システム管理者及び情報セキュリティ管理者は、利用されていない ID が放置されないよう、点検しなければならない。

3　統括情報システム管理者及び情報セキュリティ管理者は、不要なアクセス権限が付与されてい

ないか定期的に確認しなければならない。

(特権を付与されたIDの管理等)

第83条　統括情報システム管理者は、市の情報システムの基本ソフトウェアの管理者権限等の特権を付与されたID及びパスワードを管理しなければならない。

2　情報セキュリティ管理者は、所管する情報システムの管理者権限等の特権を付与されたID及びパスワードについて、次に掲げるとおり管理しなければならない。

(1)　管理者権限等を利用する者を必要最小限にし、管理者権限等を付与したID及びパスワードの漏えい等が発生しないよう、厳重に管理すること。

(2)　管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じること。

(3)　管理者権限等を付与したID及びパスワードの変更は、原則として委託事業者に行わせないこと。

(4)　管理者権限等を付与したID及びパスワードについて、人事異動の際のパスワードの変更や入力回数制限等のセキュリティ機能を強化すること。

(5)　管理者権限等を付与したIDを初期設定以外のものに変更すること。

(職員等による外部からのアクセス等の制限)

第84条　情報セキュリティ管理者は、市が管理するネットワーク及びサーバ等に外部からアクセスする仕組みを構築する場合、最高情報セキュリティ責任者の許可を得なければならない。

2　最高情報セキュリティ責任者は、市の管理するネットワーク及びサーバ等に対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

3　最高情報セキュリティ責任者は、第1項に規定する許可を与えようとするときには、情報セキュリティ管理者に対し、次に掲げる措置を講じるよう指示しなければならない。

(1)　端末の利用者の認証

(2)　IPアドレス及び電話番号等によるアクセスの制限

(3)　アクセス時間の限定

(4)　管理簿による利用者の管理

(5)　通信の暗号化

(6)　その他最高情報セキュリティ責任者が必要と認める事項

4　情報セキュリティ管理者は、外部とのアクセスに利用する端末を職員等に貸与する場合、管理簿による持出し管理等セキュリティ確保のために必要な措置を講じなければならない。

5　職員等は、外部から持ち込んだ記録媒体を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないことを確認しなければならない。

(自動識別の設定)

第85条　統括情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

(ログイン時の表示等)

第 86 条　情報セキュリティ管理者は、サーバ等へのログインについて、可能な限り、次に掲げるとおり適切な情報セキュリティ対策を施すとともに、その手順を定めなければならない。

(1)　ログイン時に表示されるメッセージの設定(ログイン試行回数の制限や直近に使用された日時の表示等)

(2)　ログインの試行回数の制限

(3)　ログイン可能時間の制限

(認証情報の管理)

第 87 条　情報セキュリティ管理者は、職員等の認証情報を厳重に管理しなければならない。

2　情報セキュリティ管理者は、職員等の認証情報について、情報セキュリティ確保のために、次に掲げる必要な措置を可能な限り講じなければならない。

(1)　職員等への仮パスワード発行によるパスワードの安全な設定

(2)　機器等の出荷時、情報システムの導入時等にあらかじめ設定されているパスワードの変更

(3)　職員等のパスワードに対する妥当性の調査

(4)　不適切なパスワードの入力を制限する機能等の導入

(5)　パスワード情報の暗号化

(管理者権限による接続時間の制限)

第 88 条　情報セキュリティ管理者は、管理者権限によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

第 3 節　システム開発、導入及び保守等

(機器等の調達に係る運用規程の整備)

第89条　統括情報セキュリティ責任者は、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。

2　統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。

(機器等及び情報システム調達時のセキュリティ機能の確認)

第89条の2　情報セキュリティ管理者は、情報システムの開発、導入及び保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

(情報システム開発時等の事故及び不正行為対策)

第 90 条　情報セキュリティ管理者は、情報システムの開発、導入及び保守における事故及び不正行為対策のため、次に掲げる事項を実施しなければならない。

(1)　責任者及び監督者を定めること。

(2)　作業者及び作業範囲を明確にすること。

(3)　開発のための方針及び手順を定めること。

(4)　開発及び保守における事故及び不正行為に関するリスク分析を行うこと。
(5)　開発、導入及び保守を行う場合、情報セキュリティ上の問題となるおそれがあるソフトウェアを使用しないこと。
(6)　機器の搬出入を管理すること。
(7)　機器等について、予防保守(機器等の障害発生を事前に想定した上での交換、定期的なクリーニング等により、障害を未然に防止すること。)を実施すること。

2　情報セキュリティ管理者は、情報システムの開発、導入及び保守における責任者及び作業者のIDの管理について、次に掲げる事項を遵守しなければならない。
(1)アクセス権限を明確にすること。
(2)当該開発又は保守終了後に不要となった時点で速やかにIDを削除すること。

(開発に用いるハードウェア及びソフトウェアの管理)

第91条　情報セキュリティ管理者は、情報システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定し、それ以外のものを利用させてはならない。

2　情報セキュリティ管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

(アプリケーション・コンテンツの開発時の対策)

第91条の2　情報セキュリティ管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

(開発環境と運用環境の分離及び移行手順の明確化)

第92条　情報セキュリティ管理者は、情報システムの開発、保守及びテスト環境と運用環境を可能な限り分離しなければならない。

2　情報セキュリティ管理者は、情報システムの開発、導入及びテスト環境から運用環境への移行について、情報システムの開発及び保守計画の策定時に手順を明確にしなければならない。

3　情報セキュリティ管理者は、開発環境から運用環境への移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

4　情報セキュリティ管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

(開発時等のテスト)

第93条　情報セキュリティ管理者は、開発した情報システムについて十分な試験を行わなければならない。

2　前項の試験において運用テストを行う場合は、あらかじめ疑似環境による操作確認を行わなければならない。

3　情報セキュリティ管理者は、個人情報等の重要な情報が含まれるデータを試験に利用してはならない。ただし、特別の理由がある場合には、統括情報システム管理者の許可を得ることにより利用することができる。

4　前項の試験において重要な情報が含まれるデータを利用する場合は、データのマスキングを行

い、試験終了後に必ずデータを消去しなければならない。

5　情報セキュリティ管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

(機器等の納入時又は情報システムの受入れ時)

第 93 条の 2　情報セキュリティ管理者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、調達仕様書等定められた検査手続に従い、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。

2　情報セキュリティ管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

(情報システムの基盤を管理又は制御するソフトウェア導入時の対策)

第 93 条の 3　情報セキュリティ管理者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。

(1)　情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順

(2)　情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

(情報システムの基盤を管理又は制御するソフトウェア運用時の対策)

第 93 条の 4　情報セキュリティ管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

(開発等に関連する資料等の整備及び保管)

第 94 条　情報セキュリティ管理者は、情報システムの開発、導入及び保守の記録を残さなければならない。

(1)　情報セキュリティ管理者は、情報システムを新規に構築し、又は更改する際には、情報システム台帳のセキュリティ要件に係る内容を記録又は記載し、当該内容について統括情報システム管理者に報告しなければならない。

(2)　情報セキュリティ管理者は、所管する情報システムの情報セキュリティ対策を実施するために必要となる文書として、以下を全て含む実施手順を整備しなければならない。

ア　情報システム構成要素ごとの情報セキュリティ水準の維持に関する手順

イ　情報セキュリティインシデントを認知した際の対処手順

ウ　情報システムが停止した際の復旧手順

2　情報セキュリティ管理者は、情報システムの開発及び保守に関する資料、マニュアル、試験データ及びテスト結果等情報システム関連文書を定められた場所に一定期間保管しなければならない。

3　情報セキュリティ管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

（情報システムにおける入出力データの正確性の確保）

第 95 条　情報セキュリティ管理者は、情報システムに入力するデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

2　情報セキュリティ管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施しなければならない。

(1)　利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーション及びウェブコンテンツの提供方式等を見直ししなければならない。

(2)　運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。

(3)　ウェブアプリケーションやウェブコンテンツにおいて、故意若しくは過失により情報が改ざんされ、又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

3　情報セキュリティ管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

4　前項において、出力されることを確実にするために、可能な限り次に掲げる事項を実施しなければならない。

(1)　出力データの妥当性を確認するための試験

(2)　データの出力処理工程の明確化

（情報システムの変更履歴の作成）

第 96 条　情報セキュリティ管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（開発及び保守用のソフトウェアの更新等）

第 97 条　情報セキュリティ管理者は、ソフトウェア（修正プログラムを含む。）の更新を行う場合、情報システムに影響を与えないか調査しなければならない。

2　情報セキュリティ管理者は、前項の結果を受けてソフトウェアの更新を速やかに行わなければならない。

（情報システム更新又は統合時の検証等）

第 98 条　情報セキュリティ管理者は、情報システムの更新又は統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新又は統合後の業務運営体制の検証を行わなければならない。

（情報システムについての対策の見直し）

第 98 条の 2　情報セキュリティ管理者は、対策の推進計画等に基づき情報システムの情報セキュリティ対策を適切に見直さなければならない。また、市役所内で横断的に改善が必要となる情報セキュリティ対策の見直しによる改善指示があった場合は、指示に基づき、情報セキュリティ対策を適切に見直さなければならない。

第 4 節　不正プログラム対策

（統括情報セキュリティ責任者の不正プログラム対策）

第 99 条　統括情報セキュリティ責任者は、不正プログラム対策（コンピュータウイルス対策等）に

関し、次に掲げる事項を実施しなければならない。

(1)　不正プログラム対策の方法及び感染時の対応計画等を作成し、情報セキュリティ管理者への周知を行うこと。

(2)　情報セキュリティ管理者による不正プログラム対策の実施状況を適宜確認し、改善が必要なものについて改善を指導すること。

(3)　不正プログラムに関する情報を収集すること。

(4)　前号により収集されたもののうち、職員等の啓発及び被害の未然防止等に効果的なものについては、職員等への周知を行うこと。

(5)　修正プログラムやバージョンアップ等の開発元のサポートが終了したソフトウェアを業務で使用しないよう、情報セキュリティ管理者に指導すること。

(情報セキュリティ管理者の不正プログラム対策)

第 100 条　情報セキュリティ管理者は、不正プログラム対策に関し、次に掲げる事項を実施しなければならない。

(1)　所管の情報システムにおける不正プログラム対策の実施状況を定期的に統括情報セキュリティ責任者に報告すること。

(2)　サーバ等における不正プログラムのチェック状況を確認すること。

(3)　不正プログラムをチェックするためのパターンファイルは、常に最新のものに保つこと。

(4)　不正プログラムへの感染が確認された場合は、緊急時対応計画に従って適切に対処すること。

(5)　所属組織の職員等に対し、不正プログラム対策に関する啓発を行うこと。

(職員等の不正プログラム対策)

第 101 条　職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

(1)　差出人が不明な電子メール又は不自然に添付されたファイルは開かないこと。

(2)　統括情報セキュリティ責任者が提供する不正プログラム情報を常に確認すること。

(3)　外部からデータ又はソフトウェアを取り入れる場合には、定められた方法により不正プログラムのチェックを行うこと。

(4)　不正プログラム対策ソフトウェアの設定を変えないこと。

(5)　不正プログラムチェックの実行を途中で止めないこと。

(6)　不正プログラムの感染が認められた場合は、直ちに情報システムの利用を中止し、情報セキュリティ管理者に連絡すること。

(専門家の支援体制)

第 102 条　統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

第 5 節　不正アクセス対策

(統括情報セキュリティ責任者の不正アクセス対策)

第 103 条　統括情報セキュリティ責任者は、不正アクセス対策として、次の事項を措置しなければならない。

(1)　使用されていないポートを閉鎖すること。

(2)　不要なサービスについて、機能を削除　又は停止すること。

(3)　不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、情報セキュリティ管理者へ通報するよう、設定しなければならない。

(攻撃への対応)

第 104 条　最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合、外部接続回線の切断等、システムの停止を含む必要な措置を講じなければならない。また、総務省や県等と連絡を密にして情報の収集に努めなければならない。

(攻撃の記録の保存)

第 105 条　最高情報セキュリティ責任者及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

(内部からの攻撃の監視)

第 106 条　統括情報システム管理者及び情報セキュリティ管理者は、職員等及び委託事業者が使用している端末又は記録媒体から、庁内のサーバ等に対する攻撃及び外部のサイトに対する攻撃が行われていないことを監視しなければならない。

(職員等による不正アクセスへの処置)

第 107 条　統括情報システム管理者及び情報セキュリティ管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する情報セキュリティ管理者に通知し、適正な処置を求めなければならない。

(サービス不能攻撃への対策)

第 108 条　統括情報システム管理者及び情報セキュリティ管理者は、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

(標的型攻撃への対策)

第 109 条　統括情報システム管理者及び情報セキュリティ管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、職員教育等の人的対策を講じなければならない。

2　標的型攻撃による組織内部への侵入を低減する対策（入口対策）や、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び外部対策）を講じなければならない。

第 6 節　セキュリティ情報の収集

(セキュリティ情報の収集及び周知等)

第 110 条　統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティ技術の向上及び情報セキュリティインシデント発生時の対応方法等に関する情報の収集に努めなければならない。

2　統括情報システム管理者及び情報セキュリティ管理者は、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなけれ

ばならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

3　統括情報セキュリティ責任者は、緊急度の高い情報及び職員等にとって必要な情報を、すべての職員等に周知しなければならない。

4　情報セキュリティ管理者は、第1項により収集した情報を、必要に応じ関係者間で共有しなければならない。

(新たなセキュリティ脅威への対策)

第111条　統括情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティに関する社会環境又は技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

第8章　運用

第1節　情報システムの監視

(情報システムの運用・保守時の対策)

第112条　統括情報システム管理者及び情報セキュリティ管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

2　統括情報システム管理者及び情報セキュリティ管理者は、情報システムの情報セキュリティ対策について、新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

3　統括情報システム管理者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムについて、情報セキュリティインシデント発生時に適切な対処が行えるよう運用をしなければならない。

(情報システムの監視機能)

第112条の2　統括情報システム管理者及び情報セキュリティ管理者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

2　統括情報システム管理者及び情報セキュリティ管理者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

3　統括情報システム管理者及び情報セキュリティ管理者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

4　統括情報システム管理者及び情報セキュリティ管理者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

(情報システムの監視)

第112条の3　統括情報システム管理者及び情報セキュリティ管理者は、情報セキュリティに関する事案を検知するため、次に掲げる情報システムの監視を行わなければならない。

(1)　重要なファイル及び情報資産等の改ざんを検出するための監視

(2)　サーバ等への不正侵入を検出するための監視

(3)　急激な通信量の増大を検出するための監視

(4)　サーバ等の資源の使用量を把握するための監視

2　統括情報システム管理者及び情報セキュリティ管理者は、外部と常時接続する場合、侵入検知システムによる監視を行わなければならない。

3　統括情報システム管理者及び情報セキュリティ管理者は、監視により得られた結果(アクセスログ及び電子メールの送受信記録等)について、消去及び改ざんされないために必要な措置を講じ、安全な場所に保管しなければならない。

4　統括情報システム管理者及び情報セキュリティ管理者は、正確な監視結果を得るため、情報システムの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

第2節　情報セキュリティポリシーの遵守状況

(遵守状況の確認及び対処)

第113条　情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、直ちに統括情報セキュリティ責任者に報告しなければならない。

2　統括情報セキュリティ責任者は、発生した問題について適正かつ直ちに対処したうえで、委員会に報告しなければならない。

3　統括情報システム管理者及び情報セキュリティ管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

(端末等の利用状況調査)

第114条　委員会から指名された者は、不正アクセス又は不正プログラム等の調査のために、職員等が使用している端末及び記録媒体等のログ及び電子メールの送受信記録等の利用状況を調査することができる。

(職員等の報告義務)

第115条　職員等は、情報セキュリティポリシーに対する違反行為を確認した場合、直ちに情報セキュリティ管理者に報告を行わなければならない。

2　前項の違反行為が、直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合、職員等は、緊急時対応計画に従って適切適正に対処しなければならない。

第3節　侵害時の対応

(緊急時対応計画)

第116条　情報セキュリティインシデント若しくは情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合は、連絡、証拠保全、被害拡大の防止、復旧及び再発防止等の措置を迅速かつ適正に実施するため、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

(緊急時対応計画に盛り込むべき内容)

第117条　緊急時対応計画には、次の事項を定めなければならない。

(1)　関係者の連絡先

(2)　発生した事案に係る報告すべき事項
(3)　発生した事案への対応措置
(4)　再発防止措置の策定

（業務継続計画との整合性確保）

第 118 条　委員会は、自然災害及び大規模かつ広範囲にわたる疾病等の事態に備えて、情報セキュリティポリシーにとどまらない危機管理規定として業務継続計画の策定について検討する必要がある。

2　前項の業務継続計画を策定するときには、情報セキュリティポリシーとの整合性を確保しなければならない。

(緊急時対応計画の見直し)

第 119 条　委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

第 4 節　例外措置

(例外措置の許可)

第 120 条　情報セキュリティ管理者は、行政事務を遂行するために情報セキュリティ関係規定を遵守することが困難な状況であり、行政事務の適正な遂行を継続するため、当該規定とは異なる方法を採用する、又は当該規定を実施しないことについて合理的な理由がある場合には、統括情報セキュリティ責任者の許可を得て、例外措置を講じることができる。

2　情報セキュリティ管理者は、行政事務の遂行に緊急を要する等の場合であって、当該規定と異なる方法を採用することが不可避のときは、統括情報セキュリティ責任者の許可を得ることなく例外措置を講じることができる。ただし、例外措置を実施後速やかに統括情報セキュリティ責任者に報告しなければならない。

3　統括情報セキュリティ責任者は、前各項において許可した例外措置の内容を、委員会に報告しなければならない。

4　前項において委員会は、例外措置の申請書及び審査結果を適正に保管しなければならない。

第 5 節　法令遵守

(関係法令等の遵守)

第 121 条　職員等は、職務の遂行において使用する情報資産を保護するため、次に掲げる法令等のほか、関係法令を遵守し、これに従わなければならない。

(1)　地方公務員法(昭和 25 年法律第 261 号)
(2)　不正アクセス行為の禁止等に関する法律(平成 11 年法律第 128 号)
(3)　著作権法(昭和 45 年法律第 48 号)
(4)　個人情報の保護に関する法律(平成 15 年法律第 57 号)
(5)　行政手続における特定の個人を識別するための番号の利用等に関する法律(平成25年法律第27号)
(6)　サイバーセキュリティ基本法（平成 26 年法律第 104 号)
(7)　笛吹市個人情報保護法施行条例（令和 4 年笛吹市条例第 29 号)

2　前項各号に掲げるもののほか、使用するソフトウェアの使用許諾契約を遵守しなければならな

い。

第 6 節　懲戒処分等

(懲戒処分)

第 122 条　情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性及び発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

(違反時の対応)

第 123 条　統括情報セキュリティ責任者が職員等の情報セキュリティポリシーに対する違反行為を確認した場合は、直ちに当該職員等が所属する課等の情報セキュリティ管理者に報告し、適正な措置を求めなければならない。

2　情報セキュリティ管理者等が職員等の情報セキュリティポリシーに対する違反行為を確認した場合は、直ちに当該職員等が所属する課等の情報セキュリティ管理者に報告し、適正な措置を求めなければならない。

3　情報セキュリティ管理者は、前各項の報告による違反行為について適正に対処したうえで、速やかに統括情報セキュリティ責任者に報告しなければならない。

4　情報セキュリティ管理者の指導によっても職員等の情報セキュリティポリシーに対する違反行為が改善されない場合、統括情報セキュリティ責任者は、統括情報システム管理者に命じて当該職員等のネットワーク又は情報システムを使用する権利を停止し、若しくは剥奪することができる。

5　前項において、統括情報セキュリティ責任者は、職員の権利を停止又は剥奪した旨を最高情報セキュリティ責任者及び当該職員が所属する課等の情報セキュリティ管理者へ通知しなければならない。

6　情報セキュリティ管理者は、第 1 項及び第 2 項の報告による違反行為が情報漏えい等の情報セキュリティ上重大な影響を及ぼす可能性があると判断した場合は、直ちに緊急時対応手順に従って適正に対処しなければならない。

第 9 章　業務委託と外部サービス(クラウドサービス)の利用

第 1 節　業務委託

(業務委託に係る運用規程の整備)

第 124 条　統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。

(1)　委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）

(2)　委託事業者の選定基準。

(業務委託実施前の対策)

第125条　情報セキュリティ管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。

(1)　委託する業務内容の特定

(2)　委託事業者の選定条件を含む仕様の策定

(3)　仕様に基づく委託事業者の選定

(4)　情報セキュリティ要件を明記した契約の締結（契約項目）

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。

ア　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

イ　個人情報漏えい防止のための技術的安全管理措置に関する取り決め

ウ　委託事業者の責任者、委託内容、作業者の所属、作業場所の特定

エ　提供されるサービスレベルの保証

オ　委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法

カ　委託事業者の従業員に対する教育の実施

キ　提供された情報の目的外利用及び委託事業者以外の者への提供の禁止

ク　業務上知り得た情報の守秘義務

ケ　再委託に関する制限事項の遵守

コ　委託業務終了時の情報資産の返還、廃棄等

サ　委託業務の定期報告及び緊急時報告義務

シ　市による監査、検査

ス　市による情報セキュリティインシデント発生時の公表

セ　情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

(5)　委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結

2　情報セキュリティ管理者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。

(1)　仕様に準拠した提案

(2)　契約の締結

(3)　委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結。

（業務委託実施期間中の対策）

第125条の2　情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。

(1)　委託判断基準に従った重要情報の提供

(2)　契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施

(3)　情報セキュリティ責任者へ措置内容の報告（重要度に応じて統括情報セキュリティ責任者及び最高情報セキュリティ責任者へ報告）

(4)　委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

2　情報セキュリティ管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。

(1)　情報の適正な取扱いのための情報セキュリティ対策
(2)　契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
(3)　委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処

(業務委託終了時の対策)

第125条の3　情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。
(1)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
(2)　委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認

2　情報セキュリティ管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。
(1)　業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
(2)　提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

第2節　情報システムに関する業務委託

(情報システムに関する業務委託における共通的対策)

第126条　情報セキュリティ管理者は、情報システムに関する業務委託の実施までに、情報システムに市の意図しない変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。

(情報システムの構築を業務委託する場合の対策)

第126条の2　情報セキュリティ管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。
(1)　情報システムのセキュリティ要件の適切な実装
(2)　情報セキュリティの観点に基づく試験の実施
(3)　情報システムの開発環境及び開発工程における情報セキュリティ対策

(情報システムの運用・保守を業務委託する場合の対策)

第126条の3　情報キュリティ管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。

2　情報キュリティ管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めなければならない。

(情報システムの一部の機能を提供するサービスを利用する場合の対策)

第126条の4　情報セキュリティ管理者は、外部の一般の者が提供する、重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サー

ビス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

2　情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

3　情報セキュリティ管理者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

4　情報セキュリティ管理者は業務委託サービスを利用する場合には、情報セキュリティ責任者へ当該サービスの利用許可を得なければならない。

第３節　外部サービス（クラウドサービス）の利用（重要性分類Ｂ以上の情報を取扱う場合

（クラウドサービスの選定に係る手順の整備）

第127条　情統括情報セキュリティ責任者は、重要性分類Ｂ以上の情報を取扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の選定に関する手順を整備しなければならない。

(1)　クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下本節において「クラウドサービス利用判断基準」という。）

(2)　クラウドサービス提供者の選定基準

(3)　クラウドサービスの利用申請の許可権限者と利用手続

(4)　クラウドサービスの利用状況の管理

（クラウドサービスの利用に係る手順の整備）

第127条の2　情統括情報セキュリティ責任者は、重要性分類Ｂ以上の情報を取扱う場合、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービス（重要性分類Ｂ以上の情報を取扱う場合）の利用に関する手順を整備しなければならない。

(1)　クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針

(2)　クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針

(3)　以下を全て含むクラウドサービスの利用を終了する際のセキュリティ対策の基本方針

ア　クラウドサービスの利用終了時における対策

イ　クラウドサービスで取り扱った情報の廃棄

ウ　クラウドサービスの利用のために作成したアカウントの廃棄

（クラウドサービスの選定）

第128条　情報セキュリティ管理者は、取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス利用判断基準に従って、業務に係る影響度等を検討した上でクラウドサービスの利用を検討しなければならない。

2　情報セキュリティ管理者は、クラウドサービスで取り扱う情報の格付及び取扱制限を踏まえ、クラウドサービス提供者の選定基準に従ってクラウドサービス提供者を選定しなければならない。また、以下の内容を含む情報セキュリティ対策をクラウドサービス提供者の選定条件

に含めなければならない。

(1)　クラウドサービスの利用を通じて市が取り扱う情報の、外部サービス提供者における目的外利用の禁止

(2)　クラウドサービス提供者における情報セキュリティ対策の実施内容及び管理体制

(3)　クラウドサービスの提供に当たり、クラウドサービス提供者又はその従業員、再委託先又はその他の者によって、市の意図しない変更が加えられないための管理体制

(4)　クラウドサービス提供者の資本関係・役員等の情報、クラウドサービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所や地域の指定

(5)　情報セキュリティインシデントへの対処方法

(6)　情報セキュリティ対策その他の契約の履行状況の確認方法

(7)　情報セキュリティ対策の履行が不十分な場合の対処方法

3　情報セキュリティ管理者は、クラウドサービスの中断や終了時に円滑に業務を移行するための対策を検討し、クラウドサービス提供者の選定条件に含めなければならない。

4　情報セキュリティ管理者は、クラウドサービスの利用を通じて市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容をクラウドサービス提供者の選定条件に含めなければならない。

(1)　情報セキュリティ監査の受入れ

(2)　サービスレベルの保証

5　情報セキュリティ管理者は、クラウドサービスの利用を通じて市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価してクラウドサービス提供者を選定し、必要に応じて市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めなければならない。

6　情報セキュリティ管理者は、クラウドサービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、クラウドサービス提供者の選定条件で求める内容をクラウドサービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を市に提供し、市の承認を受けるよう、クラウドサービス提供者の選定条件に含めなければならない。また、クラウドサービス利用判断基準及びクラウドサービス提供者の選定基準に従って再委託の承認の可否を判断しなければならない。

7　情報セキュリティ管理者は、クラウドサービスの特性を考慮した上で、クラウドサービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、以下の内容をすべて含めたセキュリティ要件を定めなければならない。

(1)　クラウドサービスに求める情報セキュリティ対策

(2)　クラウドサービスで取り扱う情報が保存される国・地域及び廃棄の方法

(3)　クラウドサービスに求めるサービスレベル

8　統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス提供者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

（クラウドサービスの利用に係る調達・契約）

第129条　情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者の選定基準及び選定条件並びにクラウドサービスの選定時に定めたセキュリティ要件を調達仕様に含めなければならない。

2　情報セキュリティ管理者は、クラウドサービスを調達する場合は、クラウドサービス提供者及びクラウドサービスが調達仕様を満たすことを契約までに確認し、利用承認を得なければならない、また、調達仕様の内容を契約に含めなければならない。

（クラウドサービスの利用承認）

第130条　情報セキュリティ管理者は、クラウドサービスを利用する場合には、利用申請の許可権限者へクラウドサービスの利用申請を行わなければならない。

2　利用申請の許可権限者は、クラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。

3　利用申請の許可権限者は、クラウドサービスの利用申請を承認した場合は、承認済みクラウドサービスとして記録しなければならない。

（クラウドサービスを利用した情報システムの導入・構築時の対策）

第131条　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。

(1)　不正なアクセスを防止するためのアクセス制御

(2)　取り扱う情報の機密性保護のための暗号化

(3)　開発時におけるセキュリティ対策

(4)　設計・設定時の誤りの防止

2　情報セキュリティ管理者は、情報システムにおいてクラウドサービスを利用する際には、情報システム台帳及び関連文書に記録又は記載しなければならない。なお、情報システム台帳に記録又は記載した場合は、統括情報システム管理者へ報告しなければならない。

3　情報セキュリティ管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。

(1)　クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順

(2)　クラウドサービスを利用した情報システムの運用・監視中における情報セキュリティインシデントを認知した際の対処手順

(3)　利用するクラウドサービスが停止又は利用できなくなった際の復旧手順

4　情報セキュリティ管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録しなければならない。

（クラウドサービスを利用した情報システムの運用・保守時の対策）

第132条　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。

(1)　クラウドサービス利用方針の規定

(2)　クラウドサービス利用に必要な教育

(3)　取り扱う資産の管理

(4)　不正アクセスを防止するためのアクセス制御

(5)　取り扱う情報の機密性保護のための暗号化

(6)　クラウドサービス内の通信の制御

(7)　設計・設定時の誤りの防止

(8)　クラウドサービスを利用した情報システムの事業継続

2　情報セキュリティ管理者は、クラウドサービスの運用・保守時に情報セキュリティ対策を実施するために必要となる項目等で修正又は変更等が発生した場合、情報システム台帳及び関連文書を更新又は修正しなければならない。なお、情報システム台帳を更新又は修正した場合は、統括情報システム管理者へ報告しなければならない。

3　情報セキュリティ管理者は、クラウドサービスの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

4　情報セキュリティ管理者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスで発生したインシデントを認知した際の対処手順を整備しなければならない。

5　情報セキュリティ管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録しなければならない。

（クラウドサービスを利用した情報システムの更改・廃棄時の対策）

第133条　統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスの利用を終了する際のセキュリティ対策を規定しなければならない。

(1)　クラウドサービスの利用終了時における対策

(2)　クラウドサービスで取り扱った情報の廃棄

(3)　クラウドサービスの利用のために作成したアカウントの廃棄

2　情報セキュリティ管理者は、前項において定める規定に対し、クラウドサービスの利用終了時に実施状況を確認・記録すること。

第3節　クラウドサービスの利用（重要性分類Ｂ以上の情報を取扱わない場合

（クラウドサービスの利用に係る規定の整備）

第134条　統括情報セキュリティ責任者は、重要性分類Ｂ以上の情報を取扱わない場合、以下を含むクラウドサービスの利用に関する手順を整備しなければならない。

(1)　クラウドサービスを利用可能な業務の範囲

(2)　クラウドサービスの利用申請の許可権限者と利用手続
(3)　クラウドサービスの利用状況の管理
(4)　クラウドサービスの利用の運用手順

(クラウドサービスの利用における対策の実施)

第 135 条　情報セキュリティ管理者は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で重要性分類Ｂ以上の情報を取り扱わない場合のクラウドサービスの利用を申請しなければならない。また、当該クラウドサービスの利用において適切な措置を講じなければならない。

2　クラウドサービスの許可権限者は、職員等によるクラウドサービスの利用申請を審査し、利用の可否を決定しなければならない。また、承認したクラウドサービスを記録しなければならない。

第 10 章　個人情報等の取扱い

(個人番号事務における申請書の受理等)

第 136 条　職員等は、個人番号利用事務（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）（以下、「番号法」という。）第 2 条第 10 項に規定する事務をいう。以下同じ。）に係る申請書等を受理するときには、番号法等その他に定めのある場合を除き、本人(番号法第 2 条第 6 号に規定する本人をいう。以下同じ。)に個人番号の記載を求めるものとする。

2　職員等は、個人番号関係事務（番号法第 2 条第 11 項に規定する事務をいう。以下同じ。）に係る申請書等を受理するときには、利用目的を明示し、本人に個人番号の記載を求めるものとする。

3　前 2 項の規定により申請書等を受理するときは、番号法等その他に定めのある場合を除き、個人番号が本人のものであること及びその者が本人であることの確認措置を行うものとする。

4　第 1 項及び第 2 項の規定により受理した申請書等は、必要な処理を行った後は、速やかに書棚等に入れて施錠し、笛吹市文書管理規程(令和 4 年笛吹市訓令第 10 号)に基づき定める文書保管期間が経過するまで厳重に保管するものとする。

(特定個人情報ファイルの作成の制限及び保有の届出)

第 137 条　職員等は、個人番号事務を処理するために必要な場合その他番号法等に定めのある場合を除き、特定個人情報を収集し、保管し、及び必要な範囲を超えて特定個人情報ファイル（番号法第 2 条第 9 項に規定するファイルをいう。以下同じ。）を作成してはならない。

2　情報セキュリティ管理者は、個人情報ファイル（番号法第 2 条第 4 項に規定するファイルをいう。以下同じ。）及び特定個人情報ファイルを保有しようとするときには、あらかじめ、個人情報の保護に関する法律（平成 15 年法律第 57 号）（以下、個人情報保護法という。）第 74 条第 1 項各号に掲げる事項を統括個人情報管理者に届け出なければならない。届け出た事項を変更しようとするときも、同様とする。

(特定個人情報保護評価)

第 138 条　情報セキュリティ管理者は、個人番号利用事務において特定個人情報ファイルを保有

しようとするときには、保有する前に(システム用ファイルの場合はプログラミングの開始前までに)、特定個人情報保護評価を実施し、評価書を統括個人情報管理者に提出しなければならない。提出した事項を変更しようとするときも、同様とする。

2　情報セキュリティ管理者は、個人番号利用事務を取り扱う情報システムにおいて、プログラムに変更を加えようとするときは、プログラミングの前までに特定個人情報保護評価を実施し、評価書を統括個人情報管理者に提出しなければならない。

(個人情報等の持出し等の制限)

第 139 条　職員等は、業務上の目的で個人情報等を取り扱う場合であっても、情報セキュリティ管理者の指示によることなく、個人情報等が記録されている媒体の外部への持出し若しくは送付又は個人情報等の複製若しくは送信を行ってはならない。

(個人番号の提供並びに特定個人情報等の利用及び提供の制限)

第 140 条　職員等は、番号法等に定めのある場合を除き、個人番号の提供を求め、又は特定個人情報等を利用し、若しくは提供してはならない。本人の同意があるときも、同様とする。

(個人情報等の廃棄)

第 141 条　個人情報等を取り扱う職員等は、個人情報等を利用する必要がなくなったとき又は笛吹市文書管理規程に基づき定めている文書保管期間が経過したときは、速やかに当該個人情報ファイル及び特定個人情報ファイルを廃棄し、又は削除しなければならない。

(アクセス制御)

第 142 条　統括情報システム管理者及び情報セキュリティ管理者は、情報システムの利用における個人情報等にアクセスする権限を、必要最小限の職員等に限定するものとする。

2　職員等は、個人情報等を処理する権限を有する場合であっても、業務上の目的以外の目的で市が保有する個人情報等にアクセスしてはならない。

(アクセス記録)

第 143 条　統括情報システム管理者及び情報セキュリティ管理者は、情報システムの利用において個人情報等へのアクセス状況を記録し、その記録を一定の期間保存しなければならない。

2　統括情報システム管理者及び情報セキュリティ管理者は、前項の記録内容を定期に及び必要に応じて確認し、不正なアクセスを監視するものとする。

(委託先の監督)

第 144 条　情報セキュリティ管理者は、個人番号事務の全部又は一部を外部に委託する場合は、委託事業者から再委託を受ける事業者も含めて、当該委託先において、市が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行うものとする。

2　情報セキュリティ管理者は、個人番号事務の業務の委託先において当該業務の一部が再委託される場合には、当該業務において取り扱う特定個人情報等の適切な管理が図られることを確認した上で再委託の諾否を判断するものとする。

第 11 章　評価及び見直し

第 1 節　監査

（監査に係る統括責任者）

第 145 条　統括情報システム管理者は、情報セキュリティ監査を統括し、その責任者とする。

2　統括情報システム管理者は、情報資産における情報セキュリティ対策の状況について、毎年度及び必要に応じて監査を行わなければならない。

（監査の実施）

第 146 条　統括情報システム管理者は、監査を実施する場合、被監査部門から独立した者を監査委員に指名し、監査の実施を依頼しなければならない。

2　監査委員は、監査及び情報セキュリティに関する研修を受けた者でなければならない。

3　統括情報システム管理者は、監査委員に対して、毎年度及び必要に応じて監査を依頼するものとする。

4　監査委員は、前項により依頼のあった監査を実施し、監査結果を報告しなければならない。

5　被監査部門は、監査の実施に協力しなければならない。

（監査実施計画の立案）

第 147 条　統括情報システム管理者は、監査実施計画を立案し、委員会の承認を得なければならない。

（委託事業者に対する監査）

第 148 条　委託事業者に業務を委託している場合、情報セキュリティ管理者は、委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査等を定期的に又は必要に応じて行わなければならない。

（監査結果の報告及び保管）

第 149 条　統括情報システム管理者は、監査委員から提出のあった監査報告書を委員会に報告しなければならない。

2　統括情報システム管理者は、前項の監査報告書のほか、監査委員が監査において収集し、又は作成した監査証拠及び監査調書を、紛失等が発生しないように適切に保管しなければならない。

（監査結果への対応）

第 150 条　委員会は、監査の結果を受けて、指摘事項を所管する情報セキュリティ管理者に対して、当該事項への対処（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

2　監査による指摘を受けた情報セキュリティ管理者は、速やかに当該事項への対処（改善計画の策定等）をしなければならない。

3　委員会は、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

4　委員会は、監査の結果が横断的な改善が必要である場合、統括情報セキュリティ責任者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。

第 2 節　自己点検

（自己点検の実施及び報告）

第 151 条　情報セキュリティ担当者は、所管するサーバ等への擬似攻撃による脆弱性を調査し、

及び所管する情報システムの設定が適正に講じられているか定期的に確認し、情報セキュリティ管理者に報告しなければならない。

2　情報セキュリティ管理者は、前項による報告のほか、所管組織の職員等における情報セキュリティポリシーの遵守状況について定期的に確認を行い、統括情報セキュリティ責任者及び所属する組織の情報セキュリティ責任者に報告しなければならない。

3　統括情報セキュリティ責任者は、前項により報告された内容をとりまとめ、委員会に報告しなければならない。

第3節　情報セキュリティポリシーの見直し

（情報セキュリティポリシーの見直し）

第152条　委員会は、監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシーの実効性について毎年度及び重大な変化が発生した際にリスク評価を行い、これに基づく改善策を協議し、必要があると認めた場合は情報セキュリティポリシー及び実施手順を改定するものとする。

2　委員会は、横断的に改善が必要となる情報セキュリティ対策の運用見直しについて、内容に応じて実施、又は対象者に指示しなければならない。

附　則

（施行期日）

1　対策基準は、平成18年4月1日から施行する。

（公開範囲）

2　対策基準は、情報資産の利用、運用、管理又は保守に関わるすべての職員等及び委託事業者に公開するものとする。

（経過措置）

3　対策基準に基づく実施手順については、速やかに整備することとする。

4　対策基準に基づく具体的な対策については、各情報資産の運用状況等に合わせて検討を行い、速やかに実施できるよう努力するものとする。

別表１　重要性分類

市の全ての情報資産は、機密性・完全性・可用性による資産価値評価に基づき重要性分類を行う。

◎重要性分類（価値評価＝自治体機密性＋自治体完全性＋自治体可用性）

分　　類	価値評価	内　　容
重要性分類 A	8～9	機密保持を要する情報が含まれており、情報セキュリティ侵害によって市民又は行政に重大な影響を及ぼすおそれがある （例）住民情報や職員に関する個人情報等
重要性分類 B	4～7 のうち、自治体機密性の評価が 2 以上又は自治体完全性の評価が 3	情報セキュリティ侵害によって市民又は行政に影響を及ぼすおそれがある （例）機密保持を要するが日常的に使用及び閲覧しない情報や、常に正確さを要する公開情報等
重要性分類 C	3～5 のうち、自治体機密性の評価が 1 及び自治体完全性の評価が 2 以下	公開情報等であり、情報セキュリティ侵害による市民又は行政への影響がほとんどない （例）Web 掲載や広報等により公開している情報

○自治体機密性の評価（重要情報の有無）

評価レベル		基　　準
3	A	「行政文書の管理に関するガイドライン」（平成 23 年 4 月 1 日内閣総理大臣決定）に定める秘密文書
	B	漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産（データベースや台帳形式になった市民の個人情報等）
	C	基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産（職員の属性に基づく個人情報や入札予定価格等）
2		自治体機密性3に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産（政策検討に関する情報等）
1		上記以外の情報資産

○自治体完全性の評価（改ざん、誤り又は破損による影響度）

評価レベル	基　　準
3	市民や行政業務全体に大きな影響を及ぼす可能性がある
2	課内の業務遂行に影響がある
1	ほとんど影響がない

○自治体可用性の評価（利用不可能であることの影響度）

評価レベル	基　　準
3	すぐに重大な支障がでる
2	長時間でなければ問題ない
1	大きな影響はない